


FORM PTO-1390 (Modified) (REV 11-2000)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTORNEY'S DOCKET NUMBER <b>RCA 89865</b>	
<b>TRANSMITTAL LETTER TO THE UNITED STATES</b> <b>DESIGNATED/ELECTED OFFICE (DO/EO/US)</b> <b>CONCERNING A FILING UNDER 35 U.S.C. 371</b>				U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.5) <div style="font-size: 1.5em; font-weight: bold; text-align: center;">10/089905</div>	
INTERNATIONAL APPLICATION NO <b>PCT/US00/28942</b>		INTERNATIONAL FILING DATE <b>19 October 2000 (19.10.00)</b>		PRIORITY DATE CLAIMED <b>19 October 1999 (19.10.99)</b>	
TITLE OF INVENTION <b>SYSTEM AND METHOD OF VERIFYING AUTHORIZATION FOR COMMUNICATING PROTECTED CONTENT</b>					
APPLICANT(S) FOR DO/EO/US <b>David Jay Duffield and Michael Scott Deiss</b>					
Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:					
<ol style="list-style-type: none"> <li>1. <input checked="" type="checkbox"/> This is a <b>FIRST</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li>2. <input type="checkbox"/> This is a <b>SECOND</b> or <b>SUBSEQUENT</b> submission of items concerning a filing under 35 U.S.C. 371.</li> <li>3. <input checked="" type="checkbox"/> This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (24) indicated below.</li> <li>4. <input checked="" type="checkbox"/> The US has been elected by the expiration of 19 months from the priority date (Article 31).</li> <li>5. <input checked="" type="checkbox"/> A copy of the International Application as filed (35 U.S.C. 371 (c) (2))           <ol style="list-style-type: none"> <li>a. <input type="checkbox"/> is attached hereto (required only if not communicated by the International Bureau).</li> <li>b. <input type="checkbox"/> has been communicated by the International Bureau.</li> <li>c. <input checked="" type="checkbox"/> is not required, as the application was filed in the United States Receiving Office (RO/US).</li> </ol> </li> <li>6. <input type="checkbox"/> An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).           <ol style="list-style-type: none"> <li>a. <input type="checkbox"/> is attached hereto.</li> <li>b. <input type="checkbox"/> has been previously submitted under 35 U.S.C. 154(d)(4).</li> </ol> </li> <li>7. <input checked="" type="checkbox"/> Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))           <ol style="list-style-type: none"> <li>a. <input type="checkbox"/> are attached hereto (required only if not communicated by the International Bureau).</li> <li>b. <input type="checkbox"/> have been communicated by the International Bureau.</li> <li>c. <input type="checkbox"/> have not been made; however, the time limit for making such amendments has NOT expired.</li> <li>d. <input checked="" type="checkbox"/> have not been made and will not be made.</li> </ol> </li> <li>8. <input type="checkbox"/> An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).</li> <li>9. <input checked="" type="checkbox"/> An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).</li> <li>10. <input type="checkbox"/> An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).</li> <li>11. <input checked="" type="checkbox"/> A copy of the International Preliminary Examination Report (PCT/IPEA/409).</li> <li>12. <input checked="" type="checkbox"/> A copy of the International Search Report (PCT/ISA/210).</li> </ol>					
<b>Items 13 to 20 below concern document(s) or information included:</b>					
<ol style="list-style-type: none"> <li>13. <input checked="" type="checkbox"/> An Information Disclosure Statement under 37 CFR 1.97 and 1.98.</li> <li>14. <input type="checkbox"/> An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.</li> <li>15. <input checked="" type="checkbox"/> A <b>FIRST</b> preliminary amendment.</li> <li>16. <input type="checkbox"/> A <b>SECOND</b> or <b>SUBSEQUENT</b> preliminary amendment</li> <li>17. <input type="checkbox"/> A substitute specification.</li> <li>18. <input type="checkbox"/> A change of power of attorney and/or address letter.</li> <li>19. <input type="checkbox"/> A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.</li> <li>20. <input type="checkbox"/> A second copy of the published international application under 35 U.S.C. 154(d)(4).</li> <li>21. <input type="checkbox"/> A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).</li> <li>22. <input checked="" type="checkbox"/> Certificate of Mailing by Express Mail</li> <li>23. <input checked="" type="checkbox"/> Other items or information</li> </ol>					
<b>Return Postcard Receipt</b>					
<b>EXPRESS MAIL LABEL No. EV 025963067US</b>			<b>DATE: April 3, 2002</b>		

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR 1.5)		INTERNATIONAL APPLICATION NO.		ATTORNEY'S DOCKET NUMBER	
10/089905		PCT/US00/28942		RCA 89865	
24. The following fees are submitted: <b>BASIC NATIONAL FEE ( 37 CFR 1.492 (a) (1) - (5)) :</b> <input type="checkbox"/> Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO ..... <b>\$1040.00</b> <input checked="" type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO ..... <b>\$890.00</b> <input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... <b>\$740.00</b> <input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) . .... <b>\$710.00</b> <input type="checkbox"/> International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) ..... <b>\$100.00</b> <div style="text-align: right;"><b>ENTER APPROPRIATE BASIC FEE AMOUNT =</b></div>				CALCULATIONS PTO USE ONLY	
Surcharge of <b>\$130.00</b> for furnishing the oath or declaration later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).				<b>\$0.00</b>	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims -	22 - 20 =	2	x \$18.00	<b>\$36.00</b>	
Independent claims	6 - 3 =	3	x \$84.00	<b>\$252.00</b>	
Multiple Dependent Claims (check if applicable).				<input type="checkbox"/>	<b>\$0.00</b>
<b>TOTAL OF ABOVE CALCULATIONS</b>				<b>=</b>	<b>\$1,178.00</b>
<input type="checkbox"/> Applicant claims small entity status. See 37 CFR 1.27). The fees indicated above are reduced by 1/2.				<b>\$0.00</b>	
<b>SUBTOTAL</b>				<b>=</b>	<b>\$1,178.00</b>
Processing fee of <b>\$130.00</b> for furnishing the English translation later than <input type="checkbox"/> 20 <input type="checkbox"/> 30 months from the earliest claimed priority date (37 CFR 1.492 (f)).				<b>\$0.00</b>	
<b>TOTAL NATIONAL FEE</b>				<b>=</b>	<b>\$1,178.00</b>
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) (check if applicable).				<input type="checkbox"/>	<b>\$0.00</b>
<b>TOTAL FEES ENCLOSED</b>				<b>=</b>	<b>\$1,178.00</b>
				<b>Amount to be: refunded</b>	<b>\$</b>
				<b>charged</b>	<b>\$</b>
a. <input type="checkbox"/> A check in the amount of _____ to cover the above fees is enclosed. b. <input checked="" type="checkbox"/> Please charge my Deposit Account No. <u>07-0832</u> in the amount of <u>\$1,178.00</u> to cover the above fees. A duplicate copy of this sheet is enclosed. c. <input checked="" type="checkbox"/> The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. <u>07-0832</u> A duplicate copy of this sheet is enclosed. d. <input type="checkbox"/> Fees are to be charged to a credit card. <b>WARNING:</b> Information on this form may become public. <b>Credit card information should not be included on this form.</b> Provide credit card information and authorization on PTO-2038.					
<b>NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.</b>					
SEND ALL CORRESPONDENCE TO:					
Mr. Joseph S. Tripoli Patent Operations THOMSON multimedia Licensing Inc. PO Box 5312 Princeton, New Jersey 08540 US			 SIGNATURE <b>DAVID T. SHONEMAN</b> NAME <b>39,371</b> REGISTRATION NUMBER <u>April 3, 2002</u> DATE		

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : David Jay Duffield and Michael Scott Deiss  
Filed : Herewith  
For : SYSTEM AND METHOD OF VERIFYING  
AUTHORIZATION FOR COMMUNICATING PROTECTED  
CONTENT

PRELIMINARY AMENDMENT

Hon. Commissioner of Patents and Trademarks  
Box PCT  
Washington, D.C. 20231

Sir:

In the US national phase application of PCT/US00/28942 filed  
herewith, please enter the following amendments:

IN THE SPECIFICATION:

Please amend the specification as follows.

On Page 1, line 3, please insert the following paragraph:

--This application claims the benefit under 35 U.S.C. § 365 of  
International Application PCT/US00/28942, filed October 19, 2000, which was  
published in accordance with PCT Article 21(2) on April 26, 2001 in English; and  
which claims benefit of U.S. provisional application serial no. 60/160,355 filed  
October 19, 1999.--

IN THE ABSTRACT:

Please add the following Abstract.

-- A method for verifying that a source device is authorized to  
communicate otherwise protected content to a sink device in a conditional access  
system using identification codes. --

EXPRESS MAIL LABEL NO. EV 025963067US

RCA 89865

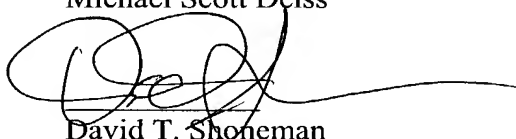
REMARKS

The specification has been amended to include a reference to the priority applications.

To meet the requirements of the United States, the Abstract (as originally filed in the PCT application) is added.

No fee is believed to have been incurred by virtue of this amendment. However if a fee is incurred on the basis of this amendment, please charge such fee against deposit account 07-0832

Respectfully submitted,  
David Jay Duffield  
Michael Scott Deiss



David T. Shoneman  
Attorney for Applicant  
Registration No. 39,371  
609/734-9875

THOMSON multimedia Licensing Inc.  
Patent Operation  
PO Box 5312  
Princeton, NJ 08543-5312  
April 3, 2002

**SYSTEM AND METHOD OF VERIFYING AUTHORIZATION FOR  
COMMUNICATING PROTECTED CONTENT**

**Field of Invention**

5       The present invention relates generally to digital audio/video transmission systems, and more particularly to a method and system for authenticating access to otherwise protected content.

**Background of Invention**

10       Extended Conditional Access (XCA) is a system for protecting digital encoded audio/video (A/V) content during transmission and storage. Under the XCA system, content of economic value is scrambled, or encrypted, to prevent unauthorized access. XCA allows recording of scrambled content, but does not permit descrambling of content that is not legitimate. Legitimate content is that which is an original or otherwise authorized by the  
15       copyright owner, for example. Of course, descrambling refers to the process of decryption. Since non-legitimate content is not descrambled, it cannot be viewed.

      A distinct characteristic of the XCA architecture is the notion of conditional access (CA) and local protection. CA specifies access to protected content, such as programming. Removable security devices perform security related functions. Content of economic value is  
20       delivered using a CA service. For example, digital satellite systems scramble video content and the descrambling keys for mass distribution to their subscribers. Some subscribers may decide to purchase the content in which case they are supplied with the necessary keys to recover/obtain the descrambling key. Those subscribers choosing not to purchase the content are not provided access to these keys. In XCA terminology, this is the process of CA.

25       XCA systems use a return channel to receive authentication of the local keys and identities that are used for accessing content. This creates a problem in that most devices need to have a return path method of some sort to make this work.

      An improved method for authenticating keys and identifiers used to access otherwise protected content in XCA and other systems which exhibit conditional access is desirable.

30

**Summary of Invention**

      A method for verifying that a source device is authorized to communicate otherwise protected content (e.g. scrambled services) to a sink device in a conditional access system, the

method including: providing substantially unique identifiers associated with the source and sink devices to a validation authority. The validation authority determines an approval code using data associated with the source and sink devices, the data corresponding to the communicated identifiers; and, the source device determines a local code using the data associated with the source and sink devices, and compares at least a portion of the approval code to at least a portion of the local code for verifying the source device is authorized to communicate the content to the sink device.

### Brief Description of the Figures

- Figure 1 illustrates a system according to one aspect of the present invention; and, Figure 2 illustrates a system according to a second aspect of the present invention.

### Detailed Description of the Invention

According to the present invention, an owner, or user or operator of devices in an XCA system is used as part of a viable return path. A major problem, however, is encountered when utilizing an operator of a device as a return channel. A user cannot be expected to read or enter a 768-bit number accurately. However, large numbers are needed to prevent brute-force cryptanalysis attacks, i.e. trying every possible signature until one works. The problem is verifying that the message, e.g. public key, received is valid. Certificates or signatures used to do this are typically at least 20 bytes in length, and are usually closer to 100 bytes. The signature must have enough possible values to make a brute force attack infeasible. According to the invention, the same goal is accomplished with a much smaller key space by limiting what resources can be used to make a brute force attack.

Figure 1 illustrates a system 10 for authenticating access to otherwise protected content. The system 10 includes a source device 20 having an associated identifier (SOURCEID), a sink device having an associated digital key (PUBLICKEY), a user or operator 50 of the source device 20, and a head end CA, or Trusted Third Party (TTP), system 40.

The source device 20 can take the form of an access device such as a satellite set-top box (STB) or media player, such as digital video cassette (DVHS) player or digital versatile disc (DVD) player, while the sink device can take the form of a digital television (DTV).

According to another aspect of the invention both the source device 20 and sink device 30 have publicly accessible serial numbers.

Generally, in order to protect the transmission of content from source device 20 to sink device 30 such that it cannot be illicitly reproduced or otherwise improperly used, the PUBLICKEY of sink device 30 is communicated to source device 20. Content provided to by source device 20 is scrambled using the PUBLICKEY of sink device 30, and transmitted to sink device 30 in scrambled form. The sink device 30 uses the corresponding private key, to unscramble the content and to enable its proper display by the sink device 30. It should also be realized that the above may be accomplished using a two stage process wherein the content is scrambled using a symmetric algorithm, and the control word for this scrambling is sent using the PUBLICKEY.

The PUBLICKEY and SOURCEID of the sink and source devices 30, 20, respectively, are determined by the TTP using the serial numbers of these devices. The determined PUBLICKEY and SOURCEID are then separately used by the devices 20, 30 and TTP to authenticate that the devices 20, 30 may operate in combination to access the content.

The user 50 obtains the serial numbers from the respective source and sink devices 20, 30 (for example, by reading them off the devices) and calls the head end CA system to enable use of the source and sink devices 20, 30 in combination. The user 50 provides these serial numbers to the head end CA system 40 as communication 52. These serial numbers can be provided in a voice communication or electronically, or acoustically for example. The Head End CA system 40 has access to a database that converts the provided serial numbers to SOURCEID and PUBLICKEY data. Hence, the head end CA system 40 can identify the SOURCEID and PUBLICKEY data of the source device 20 and sink device 30 from these communicated serial numbers, e.g. by using a lookup. According to another aspect of the present invention, it is important that the relationship between the serial numbers and SOURCEID is not public, and not readily ascertainable.

In Figure 1, the head end CA system 40 computes a hash code of these two values, e.g. the SOURCEID and PUBLICKEY as an approval hash calculation, and provides it to the user 50 as a Personal Identification Number (PIN) (illustrated as communication 42). The user 50 then enters this PIN into the source device 20 (illustrated as communication 54), which has computed the same hash, e.g., as a local hash calculation using the SOURCEID resident in the

source device 20 and PUBLICKEY provided by the sink device 30 (illustrated as communication 34). If the PIN matches the hash, then the source device 20 recognizes that the PUBLICKEY provided in communication 34 from the sink device 30 is valid for use, that the head end CA system 40 has been given this key, and that the head end CA system 40 approves it for use such that the source device 20 and sink device 30 are authorized to operate in combination with one another.

According to another aspect of the present invention, and as set forth, either the SOURCEID and/or the algorithm for computing the hash is kept secret. As will be understood by those possessing an ordinary skill in the pertinent art, the fact that a potential pirate does not have this input to the hash function effectively prevents a brute force attack with a more powerful computer.

According to another aspect of the present invention, the PIN code has a large enough space that an exhaustive search for a valid signature takes prohibitively long. One way of accomplishing this is to have the source device 20 take a significant time to approve the PIN code, either with a complex calculation, or with a waiting period after the computation, for example. A suggested value for this application, e.g., copy protection for a home A/V network, could be a 9 or 10 digit PIN, and a compute time of one second. This would force an average exhaustive search time of  $5 \times 10^8$  or  $5 \times 10^9$  seconds, or approximately 16 or 160 years.

According to an alternative aspect of the present invention, another input to the hash function can be a title code or media, such as a tape or DVD, serial number. This allows for individual titles or tapes to be approved or disapproved for use, for example. One can accomplish significant time savings by storing the serial numbers for a given user 50 in the head end CA system 40 so that the user 50 does not have to provide them for each transaction.

According to another alternative aspect of the present invention, another input to the hash function can be indicative of total running time or elapsed time since the first approval. This allows the approval to automatically expire after a set time or usage. If an extra time code is needed, this can be signaled from the source device 20 to the user 50. The time codes should be sufficiently random such that the user 50 cannot effectively guess or otherwise predict what the next time code will be. If the user 50 were capable of doing this, he could call in beforehand, and essentially pre-authorize his system by getting the PIN codes before they were required.



According to yet another alternative aspect of the present invention, another PIN code based system is based on balkanizing or dividing the key space of local networks into smaller segments without going to the security extreme of using unique per-network keys.

Figure 2 illustrates another system 100 suitable for authenticating keys and identifiers used to access otherwise protected content. The system 100 includes a source device 120 having an associated SOURCEID, a sink device 130 having an associated PUBLICKEY, a user, or operator 150 of the source device 120 and a head end CA system 140.

Sink devices can be made with a relatively small number of private keys, 10,000 for example. The user 150 reads the serial numbers of the sink device 130 and source device 120 (illustrated as communication 132, 122 respectively). The user 150 then calls into the head end CA system 140, provides the serial number of the sink device 130 and source device 120, and receives the PIN code for this sink device 130 (illustrated as communications 152, 142). The PIN code can be determined via a lookup table or appropriate calculation. The user 150 then enters this PIN code into the source device 120 (illustrated as communication 154), and the source device 120 indexes to the correct public key to use for the sink device 130 using a table of public keys 160.

The table of public keys 160 is large compared to the storage of the source device 120 itself. Table 160 is encrypted, and stored at the beginning of prerecorded media (for example, tapes). This provides an easy mechanism for obtaining the public key (PUBLICKEY) when needed, as any prerecorded tape may be used to initialize the network. After that, the system 100 will work on it's own, as the source device 120 will remember the proper key or use with the sink device 130.

Prerecorded media such as tapes are conventionally encrypted with some other, stronger encryption system. In the present invention, only the digital link from source device 120 to sink device 130 is encrypted with this weaker local key. While the local key is not unique to this network, it will be very difficult to profitably make copies of material if 10,000 different versions of the tape are required for each title.

In the event that one of the 10,000 local keys of the above-described system 100 becomes known, "pirate" users might continually use the same PIN code to allow content to be played using any source device 120. System 100 may be improved by making the PIN

WO 01/30083

PCT/US00/28942

6

code a hash function of the SOURCEID, as well as the index into the table of public keys 160. This forces the user 50 to obtain a unique PIN for each source device 120. If an overwhelming number of requests come in for a given public key in the index table 160, then that can be used as a signal that a private key has been compromised.

CLAIMS

1. A method for verifying that a source device is authorized to communicate protected content to a sink device comprising:

receiving at said source device an approval code associated with said source and sink  
5 devices;

determining, in said source device, a local code using data associated with said source and sink devices; and

comparing at least a portion of said approval code to at least a portion of said local code.

10

2. The method according to claim 1, wherein said approval code is determined based on a hash calculation using identifiers uniquely associated with said source and sink devices and wherein said local code is determined based on a hash calculation using data from said sink device and a source identifier prestored in said source device.

15

3. The method according to claim 2, wherein said data associated with said source device for determining said local code is not public information and wherein said data associated with said sink device for determining said local code is public information.

20 4. The method of Claim 2, wherein said identifiers are serial numbers or other identification codes accessible to a user, and wherein said data from said sink device used in said hash calculation is a public key.

5. A method for verifying that a source device is authorized to communicate protected  
25 content to a sink device comprising:

providing substantially unique identifiers associated with said source and sink devices to a validation authority;

receiving from said validation authority an approval code, said approval code using data corresponding to said identifiers;

5 determining, in said source device, a local code using said data associated with said source and sink devices, and

comparing at least a portion of said approval code to at least a portion of said local code.

10 6. The method of Claim 5, further comprising said validation authority providing said at least portion of said approval code to a user, and said user providing said at least portion of said approval code to said source device.

15 7. The method of Claim 5, wherein said substantially unique identifiers are provided to said validation authority by said user.

8. The method of Claim 5, wherein said source device is selected from one of an access device and a media player and wherein said sink device is a digital television.

20 9. The method of Claim 5, wherein said data associated with said source device is secured so as not to be readily ascertainable by said user.

10. The method of Claim 5, wherein said data associated with said source and sink devices comprises a unique identification indicative of said source device and a public encryption key  
25 associated with said sink device.

11. The method of Claim 10, wherein said unique identification indicative of said source device is secured from a user of said source device.
- 5 12. The method of Claim 1, further comprising said source device communicating whether said source device is authorized to provide said content to said sink device to a user, and intentionally delaying communicating whether or not said compared approval code and local code are consistent.
- 10 13. A method for authenticating at least one security key and at least one identifier used to access protected content, said method comprising:
- receiving at a first device a plurality of security keys with said content;
- receiving said identifier at said first device to be used to provide said content to a second device, said identifier being associated with said second device;
- 15       selecting one of said plurality of security keys using said first device; and,
- providing said content to said second device using said first device and selected security key.
- 20 14. The method according to claim 13, further comprising providing a serial identification indicative of said second device for accessing said content to a validation authority.
15. The method according to claim 14, further comprising determining an identifier associated with said second device using said serial identification.

16. The method of Claim 13, wherein said plurality of security codes are indexed in a table of keys and said identifier is the index of said select key in the table of keys and a result of a hash function of said identifier.

- 5 17. A method for verifying that a source device having an associated substantially unique identification and serial number and a sink device having a substantially unique key and serial number should have access to content by using a validation authority, wherein said unique identification is secured from access by a user of said source device, said method comprising:

providing said serial numbers to said validation authority;

- 10 said validation authority determining said substantially unique identifier using said serial numbers; and, if said access to said content is authorized,

said validation authority determining an authorization identifier using said substantially unique identifier;

- 15 said source device determining a local identifier using said substantially unique identifier; and,

verifying said source device and sink device should have access to content if said authorization identifier and local identifier correspond to one another.

18. The method of Claim 17, further comprising said validation authority providing said at least portion of said authorization identification to a user, and said user providing said authorization identification to said source device.
- 20

19. A method for verifying that a set top box is authorized to communicate protected content to a digital television comprising:

receiving at said set top box an approval code associated with said set top box and said  
5 digital television;

determining, in said set top box, a local code using data associated with said set top box and said digital television; and

comparing at least a portion of said approval code to at least a portion of said local code.

10

20. The method of claim 19, wherein the approval code is generated using the respective serial numbers of the set top box and the digital television.

21. A method for verifying that a digital video recorder is authorized to communicate  
15 protected content to a digital television comprising:

receiving at said digital video recorder an approval code associated with digital video recorder and said digital television;

determining, in said digital video recorder, a local code using data associated with said digital video recorder and said digital television; and

20 comparing at least a portion of said approval code to at least a portion of said local code.

22. The method of claim 21, wherein the approval code is generated using the respective serial numbers of the digital video recorder and the digital television.

25

(19) World Intellectual Property Organization  
International Bureau



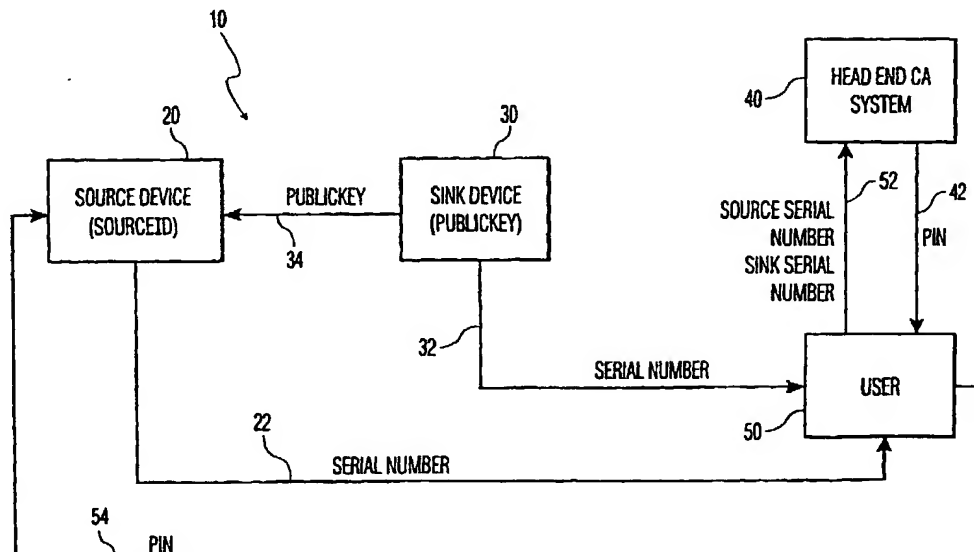
(43) International Publication Date  
26 April 2001 (26.04.2001)

PCT

(10) International Publication Number  
**WO 01/30083 A1**

- (51) International Patent Classification<sup>7</sup>: **H04N 7/167**, 7/16, 5/00
- (21) International Application Number: PCT/US00/28942
- (22) International Filing Date: 19 October 2000 (19.10.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
60/160,355 19 October 1999 (19.10.1999) US
- (71) Applicant (for all designated States except US): **THOMSON LICENSING S.A.** [FR/FR]; 46, quai Alphonse Le Gallo, F-92648 Boulogne Cedex (FR).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **DUFFIELD, David, Jay** [US/US]; 5459 Fall Creek Road, Indianapolis, IN 46220 (US). **DEISS, Michael, Scott** [US/US]; 1103 Indian Pipe Lane, Zionsville, IN 46007 (US).
- (74) Agents: **TRIPOLI, Joseph, S. et al.**; Thomson Multimedia Licensing Inc., P.O. Box 5312, Princeton, NJ 08540 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).
- Published:  
— With international search report.  
— Before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments.
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SYSTEM AND METHOD OF VERIFYING AUTHORIZATION FOR COMMUNICATING PROTECTED CONTENT



(57) Abstract: A method for verifying that a source device is authorized to communicate otherwise protected content to a sink device in a conditional access system using identification codes.

WO 01/30083 A1



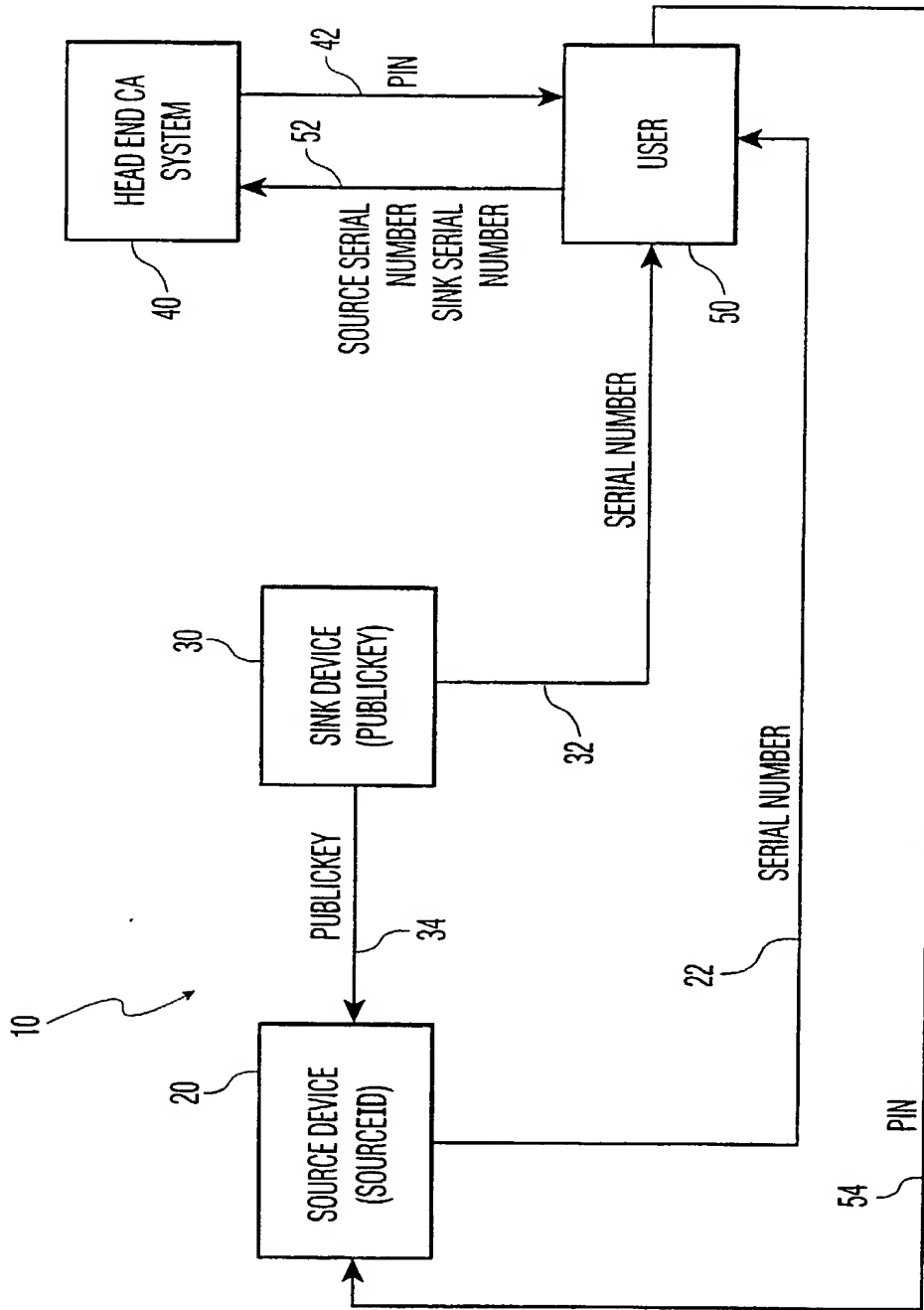


FIG. 1

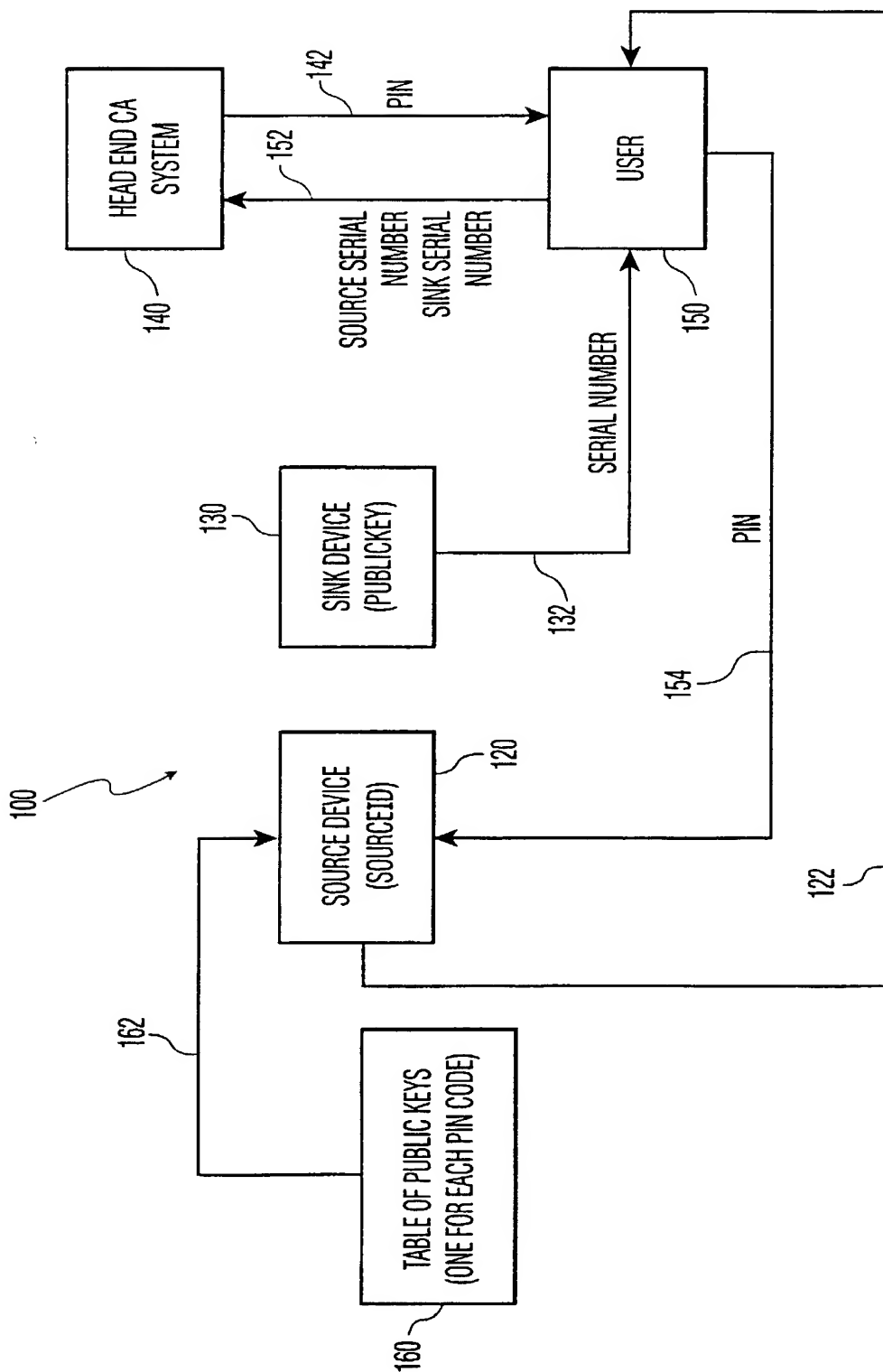


FIG. 2

EXPRESS EV 025963067US

Please type a plus sign (+) inside this box → ☐

PTO/SB/01 (10-00)

Approved for use through 10/31/2002 OMB 0651-0032  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

<b>DECLARATION FOR UTILITY OR DESIGN PATENT APPLICATION</b> <b>(37 CFR 1.63)</b>  <input type="checkbox"/> Declaration Submitted With Initial Filing <b>OR</b> <input type="checkbox"/> Declaration Submitted after Initial Filing (surcharge (37 CFR 1.16 (e)) required)	<b>Attorney Docket Number</b>	RCA 89865
	<b>First Named Inventor</b>	David Jay Duffield et al.
	<b>COMPLETE IF KNOWN</b>	
	<b>Application Number</b>	/
	<b>Filing Date</b>	
	<b>Group Art Unit</b>	
	<b>Examiner Name</b>	

As a below named inventor, I hereby declare that:

My residence, post office address, and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

SYSTEM AND METHOD OF VERIFYING AUTHORIZATION FOR COMMUNICATING PROTECTED CONTENT

the specification of which (Title of the Invention)

☐ is attached hereto

OR

☒ was filed on (MM/DD/YYYY)

October 19, 2000

as United States Application Number or PCT International

Application Number PCT/US00/28942 and was amended on (MM/DD/YYYY) 10/25/01 (if applicable).

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or of any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Country	Priority Not Claimed	Certified Copy Attached?	
					YES	NO
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Additional foreign application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto:

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date (MM/DD/YYYY)	<input type="checkbox"/> Additional provisional application numbers are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.
US 60/160,355	October 19, 1999	

[Page 1 of 2]

Burden Hour Statement: This form is estimated to take 21 minutes to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

Please type a plus sign (+) inside this box →

+

PTO/SB/01 (10-00)

Approved for use through 10/31/2002 OMB 0651-0032

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

## DECLARATION — Utility or Design Patent Application

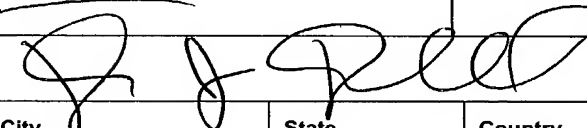
Direct all correspondence to: ☐ Customer Number or Bar Code Label ☐ OR ☐ Correspondence address below

Name	JOSEPH S. TRIPOLI		
Address	THOMSON MULTIMEDIA LICENSING INC.		
Address	PO Box 5312		
City	State	ZIP	
PRINCETON	NJ	08543-5312	
Country	Telephone	Fax	
USA	609-734-9875	(609) 734 - 9700	

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

NAME OF SOLE OR FIRST INVENTOR:

☐ A petition has been filed for this unsigned inventor

Given Name	DAVID JAY	Family Name or Surname	DUFFIELD
Inventor's Signature			Date
			3/18/2002
Residence: City	State	Country	Citizenship
Indianapolis	IN IN	US	US

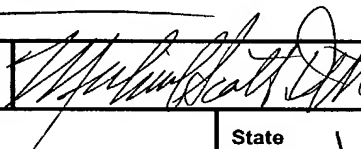
Mailing Address

Mailing Address 5459 Fall Creek Road

City	State	ZIP	Country
Indianapolis	Indiana	46220	US

NAME OF SECOND INVENTOR:

☐ A petition has been filed for this unsigned inventor

Given Name	MICHAEL SCOTT	Family Name or Surname	DEISS
Inventor's Signature			Date
			3/25/02
Residence: City	State	Country	Citizenship
Zionsville	IN IN	US	US

Mailing Address

Mailing Address 1103 Indian Pipe Lane

City	State	ZIP	Country
Zionsville	Indiana	46007	US

☐ Additional Inventors are being named on the \_\_\_\_\_ supplemental Additional Inventor(s) sheet(s) PTO/SB/02A attached hereto.